

COORDINATE SUM AND DIFFERENCE SETS OF d -DIMENSIONAL MODULAR HYPERBOLAS

AMANDA BOWER, RON EVANS, VICTOR LUO, AND STEVEN J. MILLER

ABSTRACT. Many problems in additive number theory, such as Fermat's last theorem and the twin prime conjecture, can be understood by examining sums or differences of a set with itself. A finite set $A \subset \mathbb{Z}$ is considered sum-dominant if $|A+A| > |A-A|$. If we consider all subsets of $\{0, 1, \dots, n-1\}$, as $n \rightarrow \infty$ it is natural to expect that almost all subsets should be difference-dominant, as addition is commutative but subtraction is not; however, Martin and O'Bryant in 2007 proved that a positive percentage are sum-dominant as $n \rightarrow \infty$.

This motivates the study of "coordinate sum dominance". Given $V \subset (\mathbb{Z}/n\mathbb{Z})^2$, we call $S := \{x + y : (x, y) \in V\}$ a coordinate sumset and $D := \{x - y : (x, y) \in V\}$ a coordinate difference set, and we say V is coordinate sum dominant if $|S| > |D|$. An arithmetically interesting choice of V is $\bar{H}_2(a; n)$, which is the reduction modulo n of the modular hyperbola $H_2(a; n) := \{(x, y) : xy \equiv a \pmod{n}, 1 \leq x, y < n\}$. In 2009, Eichhorn, Khan, Stein, and Yankov determined the sizes of S and D for $V = \bar{H}_2(1; n)$ and investigated conditions for coordinate sum dominance. We extend their results to reduced d -dimensional modular hyperbolas $\bar{H}_d(a; n)$ with a coprime to n .

CONTENTS

1. Introduction	2
2. Counting Preliminaries	4
3. Cardinalities of $\bar{S}_2(a; p^t)$ and $\bar{D}_2(a; p^t)$	4
3.1. Case 1: $p = 2$	4
3.2. Case 2: $p > 2$	5
3.3. Ratios for $d = 2$	6
4. Cardinality of $\bar{S}_d(m; a; n)$ for $d > 2$	8
5. Conclusion and Future Research	9
Appendix A. Additional Proofs	10
A.1. Proof of Proposition 2.1	10
A.2. Proof of Lemma 2.3	10
A.3. Proof of Theorem 3.3 cases	11
A.4. Proof of Lemma 3.4	13
A.5. Proof of Lemma 3.5	13
References	14

Date: December 13, 2012.

2010 Mathematics Subject Classification. 11P99, 14H99 (primary), 11T23 (secondary).

Key words and phrases. Modular hyperbolas, coordinate sumset, coordinate difference set.

We thank Mizan R. Khan for introducing us to this problem and for helpful discussions and comments on an earlier draft. The first and third named authors were supported by Williams College and NSF grant DMS0850577; the fourth named author was partially supported by NSF grant DMS0970067.

1. INTRODUCTION

Let $A \subset \mathbb{N} \cup \{0\}$. Two natural sets to study are

$$\begin{aligned} A + A &= \{x + y : x, y \in A\} \\ A - A &= \{x - y : x, y \in A\}. \end{aligned} \tag{1.1}$$

The former is called the sumset and the latter the difference set. Many problems in additive number theory can be understood in terms of sum and difference sets. For instance, the Goldbach conjecture says that the even numbers greater than 2 are a subset of $P + P$, where P is the set of primes. The twin prime conjecture states that there are infinitely many ways to write 2 as a difference of primes (and thus if P_N is the set of primes exceeding N , $P_N - P_N$ always contains 2). If we let A_n be the set of positive n^{th} powers, then Fermat's Last Theorem says $(A_n + A_n) \cap A_n = \emptyset$ for all $n > 2$.

Let $|S|$ denote the cardinality of a set S . A set A is sum dominant if $|A + A| > |A - A|$. We might expect that almost all sets are difference dominant since addition is commutative while subtraction is not. However, in 2007 Martin and O'Bryant [MO] proved that a positive percentage of sets are sum dominant; i.e., if we look at all subsets of $\{0, 1, \dots, n - 1\}$ then as $n \rightarrow \infty$ a positive percentage are sum dominant. One explanation is that choosing A uniformly from $\{0, 1, \dots, n - 1\}$ is equivalent to taking each element from 0 to $n - 1$ to be in A with probability $1/2$. By the Central Limit Theorem this implies that there are approximately $n/2$ elements in a typical A , yielding on the order of $n^2/4$ pairs whose sum must be one of $2n - 1$ possible values. On average we thus have each possible value realized on the order of $n/8$ ways. It turns out most possible sums and differences are realized (the expected number of missing sums and differences are 10 and 6, respectively). Thus most sets are close to being balanced, and we just need a little assistance to push a set to being sum-dominant. This can be done by carefully controlling the fringes of A (the elements near 0 and $n - 1$). Such constructions are the basis of numerous results in the field; see for example [ILMZ, MO, MOS, MPR, Zh1, Zh2].

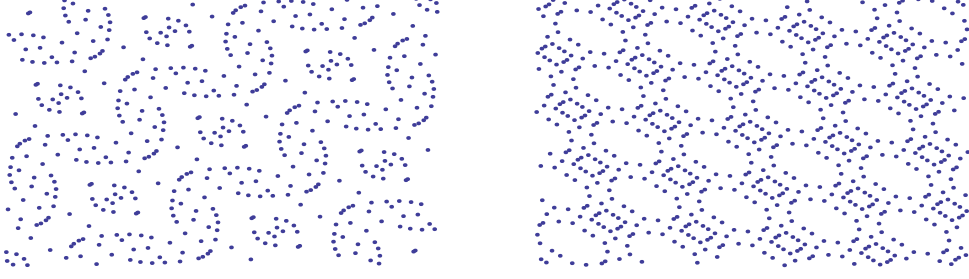
This motivates the study of “coordinate sum dominance” on fringeless sets such as $(\mathbb{Z}/n\mathbb{Z})^2$. Given $V \subset (\mathbb{Z}/n\mathbb{Z})^2$, we call $S := \{x + y : (x, y) \in V\}$ a coordinate sumset and $D := \{x - y : (x, y) \in V\}$ a coordinate difference set, and we say V is coordinate sum dominant if $|S| > |D|$. An arithmetically interesting choice of V is $\bar{H}_2(a; n)$, which is the reduction modulo n of the modular hyperbola

$$H_2(a; n) := \{(x, y) : xy \equiv a \pmod{n}, 1 \leq x, y < n\}, \tag{1.2}$$

where $(a, n) = 1$. Eichhorn, Khan, Stein, and Yankov [EKSY] determined the cardinalities of S and D for $V = \bar{H}_2(1; n)$ and investigated conditions for coordinate sum dominance. See [MV] for additional results on related problems in other modular settings.

The modular hyperbolas in (1.2) have very interesting structure, as is evidenced in Figure 1. See Figures 1 through 4 of [EKSY] for additional examples.

In the sequel, coordinate sumsets will be the only type of sumset discussed. Hence we may drop the premodifier “coordinate” without fear of confusion. For a relatively prime to n , we define the sumset $S_2(a; n)$, the difference set $D_2(a; n)$, and their reduced


 FIGURE 1. (a) Left: $H_2(51; 2^{10})$. (b) Right: $H_2(1325; 48^2)$.

counterparts as

$$\begin{aligned}
 S_2(a; n) &= \{x_1 + x_2 : (x_1, x_2) \in H_2(a; n)\} \\
 D_2(a; n) &= \{x_1 - x_2 : (x_1, x_2) \in H_2(a; n)\} \\
 \bar{S}_2(a; n) &= \{x_1 + x_2 \bmod n : (x_1, x_2) \in H_2(a; n)\} \\
 \bar{D}_2(a; n) &= \{x_1 - x_2 \bmod n : (x_1, x_2) \in H_2(a; n)\}.
 \end{aligned} \tag{1.3}$$

From a geometric viewpoint, $\#S_2(a; n)$ counts the number of lines of slope -1 that intersect $H_2(a; n)$, and $\#D_2(a; n)$ counts the number of lines of slope 1 that intersect $H_2(a; n)$. When the ratio

$$c_2(a; n) := \#\bar{S}_2(a; n) / \#\bar{D}_2(a; n) \tag{1.4}$$

exceeds 1, we have sum-dominance of $\bar{H}_2(a; n)$.

A d -dimensional modular hyperbola is of the form

$$H_d(a; n) := \{(x_1, \dots, x_d) : x_1 \cdots x_d \equiv a \bmod n, 1 \leq x_1, \dots, x_d < n\}, \tag{1.5}$$

where $(a, n) = 1$. We define the generalized signed sumset as

$$\bar{S}_d(m; a; n) = \{x_1 + \cdots + x_m - \cdots - x_d \bmod n : (x_1, \dots, x_d) \in H_d(a; n)\}, \tag{1.6}$$

where m is the number of plus signs in $\pm x_1 \pm \cdots \pm x_d$. In particular, $\bar{S}_2(1; a; n) = \bar{D}_2(a; n)$ and $\bar{S}_2(2; a; n) = \bar{S}_2(a; n)$.

The goal of this paper is to extend results of [EKSY] to the general two-dimensional modular hyperbolas in (1.2), and to investigate the higher dimensional modular hyperbolas defined in (1.5). We prove explicit formulas for the cardinalities of the sumsets $\bar{S}_2(a; n)$ and difference sets $\bar{D}_2(a; n)$ (Theorems 3.3 and 3.6). This allows us to analyze the ratios $c_2(a; n)$ (Theorems 3.8 – 3.12), thus providing conditions on a and n for sum dominance and difference dominance of reduced modular hyperbolas $\bar{H}_2(a; n)$. For example, a special case of Theorem 3.9 shows that if $a = 11$ and $n = 3^t 7^s$ with $t \geq 2$, then $c_2(a; n) > 1$, i.e., we have sum dominance. A special case of Theorem 3.12 shows that when a is a fixed power of 4, we have sum dominance for more than 85% of those n relatively prime to a . For $d > 2$ and positive integers n whose prime factors all exceed 7, we prove in Theorem 4.1 that $\#\bar{S}_d(m; a; n) = n$. This means that each such generalized sumset consists of all possible values mod n , i.e., all possible sums and differences occur.

2. COUNTING PRELIMINARIES

In this section we present some counting results that are central to proving our main theorems. Many of these are natural generalizations of results from [EKSY], so we refer the reader to the appendix for detailed proofs.

Throughout this paper, p always denotes a prime. The following proposition reduces the analysis of the cardinalities of $\bar{S}_d(m; a; n)$ to those of $\bar{S}_d(m; a; p^t)$, where p^t is a factor in the canonical factorization of n .

Proposition 2.1. *Let $n = \prod_{i=1}^k p_i^{e_i}$ be the factorization of n into distinct prime powers. Then*

$$\#\bar{S}_d(m; a; n) = \prod_{i=1}^k \#\bar{S}_d(m; a; p_i^{e_i}). \quad (2.1)$$

The proof is given in Appendix A.1.

Lemma 2.2 cuts our work in half, as once we understand the sumset we immediately have results for the corresponding difference set.

Lemma 2.2. *We have $\bar{S}_2(a; n) = \bar{D}_2(-a; n)$.*

Proof. We show $\bar{S}_2(a; n) \subseteq \bar{D}_2(-a; n)$; the reverse containment is handled similarly. Let $\tau \in \bar{S}_2(a; n)$. Then there exists $(x_0, y_0) \in H_2(a; n)$ such that $x_0 y_0 \equiv a \pmod{n}$ and $x_0 + y_0 \equiv \tau \pmod{n}$. Since $(x_0, n - y_0) \in H_2(-a; n)$ and $\tau \equiv x_0 - (n - y_0) \pmod{n}$, we see that $\tau \in \bar{D}_2(-a; n)$. \square

Lemma 2.3. *We have $(2k \bmod p^t) \in \bar{D}_2(a; p^t) \Leftrightarrow (k^2 + a)$ is a square modulo p^t . The map $f(k) = 2k \bmod p^t$ defines a bijection*

$$f : \{k : k^2 + a \text{ is a square mod } p^t, 0 \leq k < p^t\} \rightarrow \bar{D}_2(a; p^t) \quad (2.2)$$

when $p > 2$. If $p = 2$, then f defines a bijection

$$f : \{k : k^2 + a \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} \rightarrow \bar{D}_2(a; 2^t). \quad (2.3)$$

See Appendix A.2. By Lemma 2.2, a similar result for S in place of D follows by replacing a by $-a$.

3. CARDINALITIES OF $\bar{S}_2(a; p^t)$ AND $\bar{D}_2(a; p^t)$

In this section we compute the cardinalities of $\bar{S}_2(a; p^t)$ and $\bar{D}_2(a; p^t)$. We then give conditions on a and n for sum dominance and difference dominance of $\bar{H}_2(a; n)$.

3.1. Case 1: $p = 2$. We isolate a useful result that we need for the proof of the next lemma.

Proposition 3.1 (Gauss [Ga]). *For $t \geq 1$, any integer of the form $4^k(8n + 1)$ is a square mod 2^t .*

The next result is used in investigating some of the cases of Theorem 3.3.

Lemma 3.2. *Write $m = 4b + r$ with $0 \leq r \leq 3$. For $t \geq 5$, $k^2 + 3 + 8m$ is a square mod 2^t if and only if $k \equiv \pm(4r + 1) \pmod{16}$.*

Proof. We only prove the case $r = 0$, as the other proofs are similar. First assume that $k^2 + 3 + 8m$ is a square mod 2^t . Reducing mod 32, we have that $k^2 + 3 + 8m \equiv k^2 + 3 \pmod{32}$, which implies that $k \equiv \pm 1 \pmod{16}$. Conversely, assume that $k = 16l \pm 1$ for some $l \in \mathbb{Z}$. Then $k^2 + 3 + 8m = (16l \pm 1)^2 + 3 + 8(4b) \equiv 256l^2 \pm 32l + 4 + 32b \equiv 4(8(8l^2 \pm l + b) + 1) \pmod{2^t}$. Hence, by Proposition 3.1, $k^2 + 3 + 8m$ is a square mod 2^t . \square

Theorem 3.3. For $t \geq 5$,

$$\begin{aligned} \#\bar{D}_2(a; 2^t) &= \begin{cases} \frac{2^{t-4}}{3} + \frac{(-1)^{t-1}}{3} + 3 & a \equiv 7 \pmod{8} \\ 2^{t-3} & a \equiv 1, 5 \pmod{8} \\ 2^{t-4} & a \equiv 3 \pmod{8} \end{cases} \\ \#\bar{S}_2(a; 2^t) &= \begin{cases} \frac{2^{t-4}}{3} + \frac{(-1)^{t-1}}{3} + 3 & a \equiv 1 \pmod{8} \\ 2^{t-3} & a \equiv 3, 7 \pmod{8} \\ 2^{t-4} & a \equiv 5 \pmod{8}. \end{cases} \end{aligned} \quad (3.1)$$

Moreover, $\#\bar{S}_2(a; 16) = 2$ for all a , and when $t \leq 3$, we have $\#\bar{S}_2(a; 2^t) = 1$ with the exception that $\#\bar{S}_2(a; 8) = 2$ when $a \equiv 1 \pmod{4}$.

Proof. The claim for $t \leq 4$ can be checked by direct calculation, so assume $t \geq 5$. By Lemma 2.2, it is enough to prove the claims about the cardinality of $\bar{D}_2(a; 2^t)$ when $a \equiv 1, 3, 5 \pmod{8}$ and $\bar{S}_2(a; 2^t)$ when $a \equiv 1 \pmod{8}$.

We refer to the Appendix A.3 for the proofs of the results for $\bar{D}_2(a; 2^t)$ when $a \equiv 1, 5 \pmod{8}$ and for $\bar{S}_2(a; 2^t)$ when $a \equiv 1 \pmod{8}$, since these proofs are straightforward generalizations of proofs in [EKSY].

It remains to prove the result for the difference set when $a \equiv 3 \pmod{8}$. Write $a = 3 + 8m$. We consider only the case where $m \equiv 0 \pmod{4}$, since the cases $m \equiv 1, 2, 3 \pmod{4}$ are proved similarly and lead to the same result. By Lemma 3.2, we see that if $m \equiv 0 \pmod{4}$, then

$$\begin{aligned} &\#\{k : k^2 + 3 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} \\ &= \#\{1 + 16l : 0 \leq l < 2^{t-5}\} + \#\{15 + 16l : 0 \leq l < 2^{t-5}\} = 2^{t-4}. \end{aligned} \quad (3.2)$$

By Lemma 2.3, we know

$$\#\bar{D}(a; 2^t) = \#\{k : k^2 + 3 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\}. \quad (3.3)$$

Hence $\#\bar{D}_2(a; 2^t) = 2^{t-4}$. \square

3.2. Case 2: $p > 2$. For this subsection, we adopt the following notation from [EKSY]:

$$\begin{aligned} S'_2(a; p^t) &= \{k \pmod{p^t} : k^2 - a \text{ is a square mod } p^t, p \nmid (k^2 - a)\} \\ S''_2(a; p^t) &= \{k \pmod{p^t} : k^2 - a \text{ is a square mod } p^t, p \mid (k^2 - a)\} \end{aligned} \quad (3.4)$$

By Lemma 2.3,

$$\#\bar{S}_2(a; p^t) = \#S'_2(a; p^t) + \#S''_2(a; p^t) \quad (3.5)$$

Lemma 3.4. *Let p be an odd prime. Then*

$$\#\bar{S}'_2(a; p^t) = \begin{cases} \frac{(p-1)p^{t-1}}{2} & \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} & \left(\frac{a}{p}\right) = 1. \end{cases} \quad (3.6)$$

See Appendix A.4 for the proof.

Lemma 3.5. *Let p be an odd prime. If $\left(\frac{a}{p}\right) = -1$, then $\#S''_2(a; p^t) = 0$ and thus $\#S_2(a; p^t) = \frac{\phi(p^t)}{2}$. If $\left(\frac{a}{p}\right) = 1$,*

$$\#S''_2(a; p^t) = \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)}. \quad (3.7)$$

See Appendix A.5 for the proof.

Theorem 3.6. *For $t \geq 1$ and $p > 2$,*

$$\begin{aligned} \#\bar{S}_2(a, p^t) &= \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} & \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & \left(\frac{a}{p}\right) = -1 \end{cases} \\ \#\bar{D}_2(a, p^t) &= \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} & p \equiv 1 \pmod{4}, \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & p \equiv 1 \pmod{4}, \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} & p \equiv 3 \pmod{4}, \left(\frac{a}{p}\right) = -1 \\ \frac{\phi(p^t)}{2} & p \equiv 3 \pmod{4}, \left(\frac{a}{p}\right) = 1. \end{cases} \end{aligned} \quad (3.8)$$

Proof. The result follows from Lemmas 3.4, 3.5, and 2.2. \square

Corollary 3.7. *For $p \equiv 1 \pmod{4}$, $c_2(a; p^k) = 1$.*

3.3. Ratios for $d = 2$. Now that we have explicit formulas for the cardinalities of the sum and difference sets, the next natural object to study is the ratio $c_2(a; n)$ of the size of the sumset to the size of the difference set. By Corollary 3.7, we only need to consider the prime factors of n which are congruent to 3 mod 4, since the primes which are congruent to 1 mod 4 do not change $c_2(a; n)$. When $p \equiv 3 \pmod{4}$, it is sufficient to evaluate $c_2(a; p^t)$ in the case when $\left(\frac{a}{p}\right) = 1$, since $c_2(-a; p^t)$ is the reciprocal of $c_2(a; p^t)$.

Theorem 3.8. *For $p \equiv 3 \pmod{4}$ and $\left(\frac{a}{p}\right) = 1$,*

$$c_2(a; p^t) = 1 - 2 \sum_{i=0}^{\lfloor t/2 \rfloor - 1} \frac{1}{p^{2i+1}} + \frac{2}{\phi(p^t)}. \quad (3.9)$$

Proof. By Theorem 3.6,

$$\begin{aligned} c_2(a; p^t) &= \left(\frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} \right) \frac{1}{\phi(p^t)/2} \\ &= \frac{p^2 - 2p - 1}{p^2 - 1} + \frac{(-1)^{t-1}(p-1) + 3p + 3}{(p+1)\phi(p^t)}. \end{aligned} \quad (3.10)$$

Therefore,

$$\begin{aligned} c_2(a; p^t) - 1 - \frac{2}{\phi(p^t)} &= \frac{-2p}{p^2 - 1} + \frac{(-1)^{t-1}(p-1) + p + 1}{(p+1)\phi(p^t)} \\ &= \frac{-2p}{p^2 - 1} + 2 \sum_{[t/2]}^{\infty} \frac{1}{p^{2i+1}} = -2 \sum_{i=0}^{[t/2]-1} \frac{1}{p^{2i+1}}. \end{aligned} \quad (3.11)$$

□

Theorem 3.9. *Let $p < q$ be primes, both congruent to 3 mod 4, and let $s, t \geq 2$. If a is a square mod p , then $c_2(a; p^t q^s) < 1$, so we have difference dominance. If a is not a square mod p , then $c_2(a; p^t q^s) > 1$, so we have sum dominance.*

Proof. It suffices to prove the first assertion, for then the second will follow by taking the reciprocal. By Theorem 3.8, $c_2(a; p^t) < 1$. If a is a square mod q , then also $c_2(a; q^s) < 1$, so that $c_2(a; p^t q^s) = c_2(a; p^t) c_2(a; q^s) < 1$, as desired. Finally, assume that a is not a square mod q . Then it remains to show that $c_2(-a; q^s) > c_2(a; p^t)$. By Theorem 3.8, $c_2(a; p^t)$ is monotone decreasing in t . Therefore it suffices to show that $\lim_{s \rightarrow \infty} c_2(-a; q^s) > c_2(a; p^2)$. This inequality is equivalent to $1 - 2q/(q^2 - 1) > 1 - (2p - 4)/(p^2 - p)$, so we must show that $(p - 2)/(p^2 - p) > q/(q^2 - 1)$. Since the right member is a decreasing function of q , it suffices to prove this inequality when $q = p + 4$, and this is easily accomplished. □

It is not hard to show that the conclusion of Theorem 3.9 still holds in the case $s = 1$, $t \geq 2$. However, the inequalities are reversed in the case $t = 1$, $s \geq 1$.

The next three theorems are straightforward generalizations of results from [EKSY], so we omit the proofs.

Theorem 3.10. *Let $N_k = \prod_{i=1}^k p_i$, where p_i is the i^{th} prime that is congruent to 3 modulo 4. Fix a perfect square a relatively prime to all of the p_i . Then*

$$c_2(a; N_k) \asymp \log \log N_k, \quad (3.12)$$

and for any $t \geq 2$,

$$c_2(a; N_k^t) \asymp (\log \log N_k)^{-1}. \quad (3.13)$$

Theorem 3.11. *Fix an integer a . Let n run through the positive integers relatively prime to a . Then*

$$(1) \quad \frac{1}{\log \log n} \ll c_2(a; n) \ll \log \log n, \quad (3.14)$$

$$(2) \quad \limsup_{n \rightarrow \infty} c_2(a; n) = \infty \quad \text{and} \quad \liminf_{n \rightarrow \infty} c_2(a; n) = 0, \quad (3.15)$$

(3)

$$\lim_{n \rightarrow \infty} \sup \frac{\#S(a; n)}{\#D(a; n)} = \infty \quad \text{and} \quad \lim_{n \rightarrow \infty} \inf \frac{\#S(a; n)}{\#D(a; n)} = 0. \quad (3.16)$$

Theorem 3.12. *For a fixed nonzero integer a , let E_a denote the set of positive integers n relatively prime to a such that $\left(\frac{a}{p}\right) = 1$ for every prime $p \equiv 3 \pmod{4}$ dividing n . Let $C_a(L) = \{n \in E_a : c_2(a; n) > L\}$. Define $E_a(x) = \{n \in E_a : n \leq x\}$ and $C_a(L, x) = \{n \in C_a(L) : n \leq x\}$. Then the lower density of $C_a(L)$ in E_a , defined by $\liminf \#C_a(L, x)/\#E_a(x)$, satisfies the inequality*

$$\liminf_{x \rightarrow \infty} \frac{\#C_a(1, x)}{\#E_a(x)} \geq K_a \prod \left(1 - \frac{1}{p^2}\right), \quad (3.17)$$

where the product is over all primes $p \equiv 3 \pmod{4}$ for which $\left(\frac{a}{p}\right) = 1$, and where

$$K_a = \begin{cases} 1 & a \equiv 0 \pmod{2} \\ 63/64 & a \equiv 1 \pmod{8} \\ 31/32 & a \equiv 5 \pmod{8} \\ 15/16 & a \equiv 3 \pmod{4}. \end{cases} \quad (3.18)$$

Furthermore, for any constant $L > 0$, the lower density of $C_a(L)$ in E_a is positive.

For example, if a is an odd power of 2, then the lower density in (3.17) exceeds 97%. Note that if the condition $\left(\frac{a}{p}\right) = 1$ is replaced by $\left(\frac{a}{p}\right) = -1$ throughout the statement of Theorem 3.12, then by Lemma 2.2, (3.17) holds with the inequality $c_2(a; n) > 1$ replaced by $c_2(a; n) < 1$.

4. CARDINALITY OF $\bar{S}_d(m; a; n)$ FOR $d > 2$

We now turn our attention to modular hyperbolas with higher dimension ($d > 2$). Suppose that $p > 7$ for every prime p dividing n . Then Theorem 4.1 shows that the higher dimensional generalized sumsets $\bar{S}_d(m; a; n)$ all have cardinality n . In particular, this cardinality is the same for every value of m , i.e., there is no dependence on the number of plus and minus signs.

Theorem 4.1. *If the prime factors of n all exceed 7, then $\#\bar{S}_d(m; a; n) = n$.*

Proof. Let $q = p^t$ for a prime $p > 7$. By Proposition 2.1, it suffices to prove that $\#\bar{S}_d(m; a; q) = q$. We will show that for every a coprime to q and every $b \pmod{q}$, the system of congruences

$$\begin{aligned} x_1 + \cdots + x_d &\equiv b \pmod{q} \\ x_1 \cdots x_d &\equiv a \pmod{q} \end{aligned} \quad (4.1)$$

has a solution. This suffices, because x_i could be replaced by $q - x_i$ for any collection of subscripts i . If (4.1) can always be solved for $d = 3$, then it can always be solved for any $d > 3$, by setting $x_i = 1$ for $i > 3$. Thus assume that $d = 3$.

Solving (4.1) is equivalent to solving the congruence $xy(b - x - y) \equiv a \pmod{q}$ for $x, y \in (\mathbb{Z}/q\mathbb{Z})^*$. Replacing y by y^{-1} and then multiplying by y , we see that this is equivalent to solving

$$x^2 + x(y^{-1} - b) + ay \equiv 0 \pmod{q}. \quad (4.2)$$

The quadratic polynomial in x in (4.2) has discriminant

$$(-4ay^3 + b^2y^2 - 2by + 1)/y^2. \quad (4.3)$$

Let $R(y) \in (\mathbb{Z}/p\mathbb{Z})[y]$ denote the cubic polynomial in y obtained by reducing the numerator in (4.3) mod p . To solve (4.2), it remains to show that there exists $y \in (\mathbb{Z}/p\mathbb{Z})^*$ for which $R(y)$ is a non-zero square mod p ; this is because a non-zero square mod p is also a square mod q (see p. 46 of [IR]).

Suppose for the purpose of contradiction that no term in the sum

$$\sum_{y=1}^{p-1} \left(\frac{R(y)}{p} \right) \quad (4.4)$$

is equal to 1. Then since $R(y)$ has at most 3 zeros in $(\mathbb{Z}/p\mathbb{Z})^*$, we have

$$S := \sum_{y=0}^{p-1} \left(\frac{R(y)}{p} \right) = w - p, \quad (4.5)$$

for some $w \in \{1, 2, 3, 4\}$.

Let D denote the discriminant of $R(y)$. Then $D \equiv 16a(b^3 - 27a) \pmod{p}$, and so D vanishes if and only if $a \equiv (b/3)^3 \pmod{p}$. When D vanishes, it follows that $b \in (\mathbb{Z}/p\mathbb{Z})^*$ and $y = 3/(4b)$ is a simple zero of $R(y)$. We conclude that $R(y)$ cannot equal a constant times the square of a polynomial in $(\mathbb{Z}/p\mathbb{Z})[y]$. Therefore (see equation (6.0.2) in [BEW]) we can apply Weil's bound to conclude that $|S| < 2\sqrt{p}$. Together with (4.5), this yields

$$p - 2\sqrt{p} < w \leq 4, \quad (4.6)$$

which contradicts the fact that $p > 7$. \square

We remark that the conditions $p > 7$ cannot be weakened in Theorem 4.1. For example, (4.2) has no solution when $p = q = 2$, $b = 0$ and $a = 1$; when $p = q = 3$ and $b = a = 1$; when $p = q = 5$, $b = 1$ and $a = 2$; and when $p = q = 7$, $b = 0$ and $a = 3$.

5. CONCLUSION AND FUTURE RESEARCH

We generalized work of [EKSY] on the modular hyperbola $H_2(1, n)$ by examining more general modular hyperbolas $H_d(a; n)$. The two-dimensional case ($d = 2$) provided interesting conditions on a and n for sum dominance and difference dominance. On the other hand, for higher dimensions ($d > 2$), all possible sums and difference are realized when the prime factors of n all exceed 7.

The following are some topics for future and ongoing research:

- (1) We can study the cardinality of sumsets and difference sets of the intersection of modular hyperbolas with other modular objects such as lower dimensional modular hyperbolas and modular ellipses. See [HK] for work on the cardinality of the intersection of modular circles and $H_2(1; n)$.

- (2) Extend Theorem 3.9 by estimating $c_2(a; n)$ in cases where n has more than two prime factors of the form $4k + 3$.
- (3) Extend Theorem 4.1 by finding the cardinality of the generalized higher dimensional sumsets in cases where $(n, 210) > 1$.
- (4) In higher dimensions ($d > 2$), nearly every sum and difference is realized for $\bar{H}_d(a; n)$. The situation becomes more interesting if we replace $\bar{H}_d(a; n)$ by a random subset chosen according to some probability distribution depending on d . If S and D denote the corresponding sumset and difference set, we can then compare the random variables $\#S$ and $\#D$.

APPENDIX A. ADDITIONAL PROOFS

The following proofs are a natural extension of the proofs given by [EKSY], and are included for completeness.

A.1. Proof of Proposition 2.1.

Proof of Proposition 2.1. Consider

$$g : \bar{S}_d(m; a; n) \longrightarrow \prod_{i=1}^k \bar{S}_d(m; a \bmod p_i^{e_i}; p_i^{e_i}) \quad (\text{A.1})$$

defined by

$$g(x) = (x \bmod p_1^{e_1}, \dots, x \bmod p_k^{e_k}). \quad (\text{A.2})$$

We claim g is a bijection.

To show g is injective, suppose $g(x) = g(y)$. Then we have $(x \bmod p_1^{e_1}, \dots, x \bmod p_k^{e_k}) = (y \bmod p_1^{e_1}, \dots, y \bmod p_k^{e_k}) \Rightarrow x \equiv y \bmod p_i^{e_i}$ for $i = 1, \dots, k$. Thus, by the Chinese Remainder Theorem, we have that $x \equiv y \bmod n$. But $0 \leq x, y < n \Rightarrow x = y$, so g is injective.

To show g is surjective, let $(\alpha_1, \dots, \alpha_k) \in \prod_{i=1}^k \bar{S}_d(m; a \bmod p_i^{e_i}; p_i^{e_i})$. Then, for each $i \in \{1, \dots, k\}$, there exists $(x_{1_i}, \dots, x_{d_i}) \in H_d(a; p_i^{e_i})$ such that $x_{1_i} + \dots + x_{m_i} - \dots - x_{d_i} \equiv \alpha_i \bmod p_i^{e_i}$. By the Chinese Remainder Theorem, the system of congruences

$$x_r \equiv x_{r_i} \bmod p_i^{e_i} \quad (\text{A.3})$$

where $1 \leq r \leq d$ has a unique solution $x_1 = x'_1, \dots, x_d = x'_d \bmod n$. Since $x_{1_i} \dots x_{d_i} \equiv a \bmod p_i^{e_i}$ for all $i \in \{1, \dots, k\}$, we have, again by the Chinese remainder theorem, $x'_1 \dots x'_d \equiv a \bmod n$. So $g(x'_1 + \dots + x'_m - \dots - x'_d \bmod n) = (\alpha_1, \dots, \alpha_k)$, and hence g is a bijection, which completes the proof. \square

A.2. Proof of Lemma 2.3. Before proving Lemma 2.3, we state a useful lemma that is a simple observation and immediate generalization of a result from [EKSY].

Lemma A.1. *Let $(x_0, y_0) \in H_2(a; p^t)$. Then $x_0 - y_0 \equiv 2k_1 \bmod p^t$ and $x_0 + y_0 \equiv 2k_2 \bmod p^t$ for some $k_1, k_2 \in \mathbb{Z}$.*

Proof. If $p = 2$, then x_0 and y_0 are both odd since they are coprime to p^t , so their sum and difference are even. If $p \neq 2$, then 2^{-1} exists $\bmod p^t$, so $x_0 - y_0 \equiv 2k_1 \bmod p^t$ and $x_0 + y_0 \equiv 2k_2 \bmod p^t$ both have solutions. \square

Proof of Lemma 2.3. Since the proofs are similar, we only prove (1).

“ \Rightarrow ” Let $(x_0, y_0) \in H_2(a; p^t)$. By Lemma A.1, $x_0 - y_0 \equiv 2k \pmod{p^t}$ for some $k \in \mathbb{Z}$. Note $x_0 - y_0 \in \bar{D}_2(a; p)$. Upon completing the square, we obtain $k^2 + a \equiv (x_0 - k)^2 \pmod{p^t}$. Thus $k^2 + a$ is a square mod p^t .

“ \Leftarrow ” Suppose $k^2 + a$ is a square mod p^t . Then there exists $c \in \mathbb{Z}$ such that $c^2 - k^2 \equiv a \pmod{p^t}$. It follows that $(x_0, y_0) = ((c + k) \pmod{p^t}, (c - k) \pmod{p^t}) \in H_2(a; p^t)$ and $x_0 - y_0 \equiv 2k \pmod{p^t}$.

Now we show that $d_{p^t, a}$ is a bijection. If $p > 2$, then $(d_{p^t, a})^{-1}(x) = 2^{-1}x \pmod{p^t}$ is the inverse of $d_{p^t, a}(x)$.

Now suppose $p = 2$. We first show $d_{p^t, a}$ is injective. Choose $k \in \mathbb{Z}$ such that $0 \leq k < 2^{t-1}$ and $k^2 + a$ is a square mod 2^t . Consider $k_1 = (k - 2^{t-1}) \pmod{2^t}$. Then $k_1^2 + a$ is also a square mod 2^t (because $k_1^2 + a \equiv k^2 + 2(2^{t-1}) - 2^t k + a \equiv k^2 + a \pmod{2^{t-1}}$). The congruence $2x \equiv 2k \pmod{2^t}$ has exactly two distinct solutions, which must be k and k_1 . Since either k or k_1 is less than 2^{t-1} , we conclude that $d_{2^t, a}$ is injective.

To show $d_{p^t, a}$ is surjective, let $t \in \bar{D}_2(a; 2^t)$. Then by Lemma A.1 there exists $(x_0, y_0) \in H_2(a; 2^t)$ such that $x_0 - y_0 \equiv t \equiv 2k \pmod{2^t}$ for some $k \in \mathbb{Z}$. Hence, since $t = 2k$, $d_{p^t, a}(k) = t$. \square

A.3. Proof of Theorem 3.3 cases. The next proposition is from [IR] (see page 46). It gives us a quick way to count squares modulo prime powers.

Proposition A.2. *For the congruence*

$$x^2 \equiv a \pmod{p^t}$$

where p is a prime and a is an integer such that $p \nmid a$, we have the following:

- (1) *If $p \neq 2$ and the congruence $x^2 \equiv a \pmod{p}$ is solvable, then for every $t \geq 1$ the congruence $x^2 \equiv a \pmod{p^t}$ is solvable with precisely two distinct solutions.*
- (2) *If $p = 2$ and the congruence $x^2 \equiv a \pmod{2^3}$ is solvable, then for every $t \geq 3$ the congruence $x^2 \equiv a \pmod{2^t}$ is solvable with precisely four distinct solutions.*

Proof of Theorem 3.3. We break the analysis by the congruence class of a modulo 8.

Case 1: Difference set for $a \equiv 1 \pmod{8}$. By Proposition 2.3, we know

$$\#\bar{D}(a; 2^t) = \#\{k : k^2 + 1 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\}. \quad (\text{A.4})$$

We claim that

$$k^2 + 1 + 8m \text{ is a square mod } 2^t \Leftrightarrow k = 4l \text{ for some } l \in \mathbb{Z}. \quad (\text{A.5})$$

“ \Rightarrow ” Assume $k^2 + 1 + 8m$ is a square mod 2^t . Then $k^2 + 1$ is a square mod 8, which yields $k \equiv 0, 4 \pmod{8}$. Hence $k = 4l$ for some $l \in \mathbb{Z}$.

“ \Leftarrow ” Assume $k = 4l$ for some $l \in \mathbb{Z}$. We want to show $k^2 + 1 + 8m = (4l)^2 + 1 + 8m$ is a square mod 2^t . Reducing modulo 8 gives us $(4l)^2 + 1 + 8m \equiv 1 \pmod{8}$, which is a square for all l . Hence, by the second part of Proposition A.2, $(4l)^2 + 1 + 8m$ is a square mod 2^t for all l . Thus

$$\{k : k^2 + 1 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} = \{4l : 0 \leq l < 2^{t-3}\}. \quad (\text{A.6})$$

Case 2: Difference set for $a \equiv 5 \pmod 8$. Using a similar argument from above, we show that

$$k^2 + 5 + 8m \text{ is a square mod } 2^t \Leftrightarrow k = 2 + 4l \text{ for some } l \in \mathbb{Z}. \quad (\text{A.7})$$

“ \Rightarrow ” Assume $k^2 + 5 + 8m$ is a square mod 2^t . Then $k^2 + 5 + 8m \equiv k^2 + 5$ is a square mod 8, which implies $k \equiv 2, 6 \pmod 8$ or $k = 2 + 4l$ for some $l \in \mathbb{Z}$.

“ \Leftarrow ” Assume $k = 2 + 4l$ for some $l \in \mathbb{Z}$. Reducing modulo 8 gives us $(2 + 4l)^2 + 5 + 8m \equiv 4 + 16l + 16l^2 + 5 + 8m \equiv 1 \pmod 8$, which is a square for all l . Hence, by the second part of Proposition A.2, $(4l)^2 + 1 + 8m$ is a square mod 2^t for all l . Since $k = 2 + 4l$ and $0 \leq k < 2^{t-1}$ we have $0 \leq l < 2^{t-3}$. Hence

$$\{k : k^2 + 1 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} = \{4l : 0 \leq l < 2^{t-3}\}. \quad (\text{A.8})$$

Case 3: Sum set for $a \equiv 1 \pmod 8$. Assume $a \equiv 1 \pmod 8$. Thus $a = 1 + 8t$ for some $t \in \mathbb{Z}$. We show that

$$\#\{k : k^2 - 1 - 8t \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} = 2\#\{k^2 \pmod{2^{t-4}}\}. \quad (\text{A.9})$$

Let $j \in \{k : k^2 - 1 - 8t \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\}$. So $j^2 - 1 - 8t$ is a square mod 2^t . Note that $j = 2l + 1$ because if not, we can reduce mod 4 and notice that -1 is a square mod 4, which is a contradiction. Also, $(l^2 + l - 2t)$ is a square mod 2^{t-2} . Hence

$$\begin{aligned} &\{k : k^2 - 1 - 8t \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} \\ &= \#\{l : l^2 + l - 2t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-2}\}. \end{aligned} \quad (\text{A.10})$$

As

$$\begin{aligned} &\#\{l : l^2 + l - 2t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-2}, l \text{ even}\} \\ &= \#\{l : l^2 + l - 2t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-2}, l \text{ odd}\}, \end{aligned} \quad (\text{A.11})$$

we find

$$\begin{aligned} &\#\{l : l^2 + l - 2t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-2}\} \\ &= 2\#\{l : l^2 + l - 2t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-2}, l \text{ odd}\}. \end{aligned} \quad (\text{A.12})$$

If l is odd, then l^{-1} exists. Note that if $l^2 + l - 2t \equiv c^2 \pmod{2^{t-2}}$, then multiplying by l^{-1} yields $1 + l^{-1} + 2l^{-2}t \equiv l^{-2}c$, which is also a square mod 2^{t-2} . Hence

$$\#\{l : 1 + l^{-1} - 2l^{-2}t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-2}, l \text{ odd}\}. \quad (\text{A.13})$$

Since $1 + l^{-1} + 2l^{-2}t$ is even and a square, $1 + l^{-1} + 2l^{-2}t \equiv 4m^2 \pmod{2^{t-2}}$ for some m , $0 \leq m < 2^{t-4}$. Therefore

$$\#\{l : l^2 + l - 2t \text{ is a square mod } 2^{t-2}, 0 \leq l < 2^{t-1}, l \text{ odd}\} = \#\{k^2 \pmod{2^{t-4}}\}; \quad (\text{A.14})$$

the proof of this case is completed by Proposition A.3. \square

A.4. Proof of Lemma 3.4.

Proof of Lemma 3.4. Suppose $l \in \#S'_2(a; p^t)$. Then $\left(\frac{l^2-a}{p}\right) = 1$ and

$$\begin{aligned}
 \#S'_2(a; p^t) &= \frac{1}{2} \sum_{l=0, (l^2-a, p)=1}^{p^t-1} \left(\left(\frac{l^2-a}{p} \right) + 1 \right) \\
 &= \frac{1}{2} \sum_{k=0}^{p^{t-1}} \sum_{l=0, l^2 \not\equiv a \pmod p}^{p-1} \left(\left(\frac{(l+kp)^2-a}{p} \right) + 1 \right) \\
 &= \left(\sum_{l=0, l^2 \not\equiv a \pmod p}^{p-1} \left(\left(\frac{l^2-a}{p} \right) + 1 \right) \right) \frac{p^{t-1}}{2} \\
 &= \left(-1 + \sum_{l=0, l^2 \not\equiv a \pmod p}^{p-1} 1 \right) \frac{p^{t-1}}{2}, \tag{A.15}
 \end{aligned}$$

as (see for example page 63 of [IR])

$$\sum_{i=0}^{p-1} \left(\frac{i^2-a}{p} \right) = -1. \tag{A.16}$$

Substituting

$$\sum_{\substack{l=0 \\ l^2 \not\equiv a \pmod p}}^{p-1} = \begin{cases} p & \left(\frac{a}{p}\right) = 1 \\ p-2 & \left(\frac{a}{p}\right) = -1 \end{cases} \tag{A.17}$$

into (A.15) gives us the desired result. \square

A.5. Proof of Lemma 3.5. We use the following fact in our proof.

Proposition A.3 (Stangl [St]). *Let p be an odd prime. Then*

$$\#\{k^2 \pmod{p^t}\} = \frac{p^{t+1}}{2(p+1)} + (-1)^{t-1} \frac{p-1}{4(p+1)} + \frac{3}{4}.$$

When $p = 2$, we have that

$$\#\{k^2 \pmod{2^t}\} = \frac{2^{t-1}}{3} + \frac{(-1)^{t-1}}{6} + \frac{3}{2}.$$

Proof. As $\left(\frac{a}{p}\right) = -1$, the congruence $x^2 - a \equiv 0 \pmod p$ has no solutions. Therefore $\#S''_2(a; p^t) = 0$.

For the other claim, let $k \in S''_2(a; p^t)$ and assume $\left(\frac{a}{p}\right) = 1$. Then $k^2 - a \equiv p^2 m^2 \pmod{p^t}$ for some $m, 0 \leq m < p^{t-2}$. We have two cases.

Case 1: Suppose $t \leq 2$. In this case, we have $m = 0$, and since the congruence $x^2 \equiv a \pmod{p^t}$ has exactly 2 solutions, we conclude that $\#S''_2(a; p^t) = 2$.

Case 2: Suppose $t \geq 3$. Consider

$$g : S''_2(a; p^t) \rightarrow \{m^2 \pmod{p^{t-2}}\} \tag{A.18}$$

defined by $g(k) = m^2$. By Proposition A.2, for each $m^2 \in \{m^2 \bmod p^{t-2}\}$, the congruence $x^2 \equiv p^2 m^2 + a \bmod p^t$ is solvable with precisely two solutions. Hence g is surjective and each element in the image of g has exactly two distinct element in its pre-image. Therefore, since $\#S_2''(a; p^t) = \#\{m^2 \bmod p^{t-2}\}$, by Theorem A.3 we are done. \square

REFERENCES

- [BEW] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, New York, 1998.
- [EKSY] D. Eichhorn, M. R. Khan, A. H. Stein and C. L. Yankov, *Sums and Differences of the Coordinates of Points on Modular Hyperbolas*, *Integers* **9** (2009), #A3.
- [HK] S. Hanrahan and M. R. Khan, *The cardinality of the value sets modulo n of $x^2 + x^{-2}$ and $x^2 + y^2$* , in *Involve* **3** (2010), no.2, 171–182.
- [Ga] C.F. Gauss, *Disquisitiones Arithmeticae*, Art. 103.
- [IR] K. Ireland and M. Rosen, *A classical Introduction to Modern Number Theory*, second edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 2010.
- [ILMZ] G. Iyer, O. Lazarev, S. J. Miller and L. Zhang, *Generalized More Sums Than Differences Sets*, *Journal of Number Theory* **132** (2012), no. 5, 1054–1073.
- [MO] G. Martin and K. O’Bryant, *Many sets have more sums than differences*, in *Additive Combinatorics*, CRM Proc. Lecture Notes, vol. 43, AMS, Providence, RI, 2007, pp. 287–305.
- [MOS] S. J. Miller, B. Orosz and D. Scheinerman, *Explicit constructions of infinite families of MSTD sets*, *Journal of Number Theory* **130** (2010) 1221–1233.
- [MPR] S. J. Miller, S. Pegado and S. L. Robinson, *Explicit constructions of infinite families of generalized MSTD sets*, *Integers* **12** (2012), #A30.
- [MV] S. J. Miller and K. Vissuet, *Most sets are balanced in finite groups*, preprint.
- [St] W. Stangl, *Counting squares in \mathbb{Z}_n* , *Math. Mag.* **69** (1996), 285–289.
- [Zh1] Y. Zhao, *Constructing MSTD Sets Using Bidirectional Ballot Sequences*, *Journal of Number Theory* **130** (2010), no. 5, 1212–1220.
- [Zh2] Y. Zhao, *Sets Characterized by Missing Sums and Differences*, *Journal of Number Theory* **131** (2011), 2107–2134.

E-mail address: amandarg@umd.umich.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MICHIGAN-DEARBORN, DEARBORN, MI 48128

E-mail address: revans@math.ucsd.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA SAN DIEGO, LA JOLLA, CA 92093

E-mail address: victor.d.luo@williams.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

E-mail address: sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267